UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,381	10/16/2001	Daryl Carvis Cromer	RPS9 2001 0054	4259

7590 05/26/2005

IBM Corporation
Personal and Printing Systems Group Legal Dept.
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/978,381	CROMER ET AL.	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3-5, 10-11, 13-15, 20-21, 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), and further in view of Kendall (U.S. Pub. No. 2002/0144103).

Referring to claim 1:

i. Lovelace et al. teach:

A method for tracking a secure boot in a computer system, wherein the computer system comprises a plurality of devices (see figure 1, items 111-113,125; and column 2, lines 55-57). The method comprise the steps of providing a secure flash memory to store expected hash values (see figure 1, item 100; and column 5, lines 55-58) and a secure interface embedded in the computer system (see figure 1, item 140; and column 2, lines 44-47); booting the computer system via BIOS (see column 4, lines 1-6); calculating a measurement value for a device of the plurality of devices booted in the computer system (see figure 3, item 320; and column 5, lines 47-48); comparing the measurement value of each of the at least one device to the expected measurement value stored in the secure flash memory (see figure 3, item 340; and column 5, lines 59-60); if measurement values match, the integrity of the computer system is assured, and the computer is booted (see figure 3, item 350; and column 5, lines 61-62).

ii. Though Lovelace et al. teach the subject matter:

Lovelace et al. teach boot components 111-114 for booting an operating system.

Lovelace et al. also mention that a loader may load some boot components from a hard disk, a network device, and from other data sources. Lovelace et al. do not explicitly mention to use PCR (platform configuration register) and shadow PCR. However, Kendall discloses a flash memory comprising registers to store configuration data (see figure 3, item 31; and paragraph [0037], lines 2-7 of Kendall).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teaching of Kendall into the method of Lovelace et al., because it's efficient to user register to store/retrieve value.

Referring to claim 3:

i. Lovelace et al. teach:

The contents of the secure flash memory may be digitally signed using the BIOS manufacturer's signature. Before being used, the BIOS is verified using the BIOS manufacturer's public key. Once verified, the BIOS can be trusted to update the expected hash value (see column 4, lines 1-6).

ii. The limitations about using PCR and shadow PCR (b1 and b3) are addressed in claim 1 above.

Referring to claim 4:

Lovelace et al. teach:

The boot components are supplied to a hash function to calculate their hash values (see figure 3, item 320; and column 5, lines 47-48).

Referring to claim 5:

Lovelace et al. teach:

If the calculated hash value matches the expected hash value stored in the secure flash memory, the operating system is booted (see figure 3, item 350; and column 5, lines 61-67).

Referring to claim 10:

Lovelace et al. do not explicitly mention whether a computer system was booted from a cold boot, hardware boot or warm boot. However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made that a

computer system can be booted from a cold boot, hardware boot, or warm boot to reclaim system resources, and therefore can run more efficiently.

Referring to claims 11 and 21:

These claims have limitations which are similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

Referring to claims 13 and 23:

These claims have limitations which are similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

Referring to claims 14 and 24:

These claims have limitations which are similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

Referring to claims 15 and 25:

These claims have limitations which are similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

Referring to claim 20:

This claim has limitations which is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

3. Claims 2, 12, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), and further in view of Girard et al. (U.S. Pub. No. 2003/0061494).

Referring to claim 2:

Lovelace et al./Kendall do not teach TPM (Trusted Platform Module), which is a standard component in TCPA (Trusted Computing Platform Alliance).

However, Girard et al. teach to access a protected storage in a computer system via a trusted platform module(TPM) (see figure 1, item 510; and paragraph [0039], lines 4-5).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Girard et al. into the system of Lovelace et al./Kendall to provide a TPM module in a computer system to be TCPA compliant.

Referring to claims 12 and 22:

These claims have limitations which are similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

4. Claims 6, 8-9, 16, 18-19, 26, 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), and further in view of Jablon et al. (U.S. Patent No. 5,421,006).

Referring to claim 6:

i. Lovelace et al./Kendall do not teach how to restore trust in the computer system if the measurement values are different.

ii. However, Jablon et al. teach a method for protecting the integrity of a computer system at the time of booting, and disclose a way for recovering from a corrupted hard-disk boot record by providing a backup removable recovery diskette (see column 14, lines 29-31 of Jablon et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Jablon et al. invention into the system of Lovelace et al./Kendall to provide a recovery method to make the system more robust.

Referring to claim 8:

The limitations of using PCR and shadow PCR in (g) are addressed in claim 1 above.

Referring to claim 9:

i. Lovelace et al./Kendall do not specifically mention an authorized entity.

ii. However, Jablon et al. teach to allow only authorized people to access critical data (see column 14, lines 36-45 of Jablon et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Jablon et al. invention into the system of Lovelace et al./Kendall to allow only authorized entity to access critical data to enforce data integrity.

Referring to claims 16 and 26:

These claims have limitations which are similar to those of claim 6, thus they are rejected with the same rationale applied against claim 6 above.

Referring to claims 18 and 28:

These claims have limitations which are similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

Referring to claims 19 and 29:

These claims have limitations which are similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

5. Claims 7, 17, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), Jablon et al. (U.S. Patent No. 5,421,006), and further in view of Rosenthal (U.S. Patent No. 5,359,659).

Referring to claim 7:

i. Lovelace et al./Kendall/Jablon et al. do not teach to run a virus protection program as a preventative operation.

ii. However, Rosenthal teaches a method for securing an existing executable software program against infection or corruption by software viruses or the like (see figure 2, item 38; and column 11, lines 49-53 of Rosenthal).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Rosenthal invention into the system of

Lovelace et al./Kendall/Jalon et al. to provide a virus protection program in the event a boot component is corrupted, so that the system becomes more robust.

Referring to claims 17 and 27:

These claims have limitations which are similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
May 9, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100